arm

TF-PSACrypto Project Update

Feb’26

© 2026 Arm

Project Update

- Preparing for Mbed TLS 4.1/TF-PSA-Crypto1.1 LTS
  - Due end of the quarter
  - First TF-PSA-Crypto LTS
  - TF-M will use 1.1 LTS for its LTS release next quarter

- ML-DSA (PQC) support
  - Based on mldsa-native implementation
  - Initially supported via. a PSA driver interface followed by PSA API support
  - Support will be limited to pure MLDSA-87
  - TF-M will integrate once available in TF-PSACrypto1.x release
  - ML-KEM to be planned after ML-DSA support

- Bug Bounty program

- TF-PSACrypto Driver repository
  - Cryptocell driver moving from TF-M repo.

- New gatekeeper
  - Valerio from Nordic has been working closely with the maintainer team in the recent months
  - He was invited and has accepted to be a gatekeeper
  - First non-Arm gatekeeper on the project

arm

© 2026 Arm

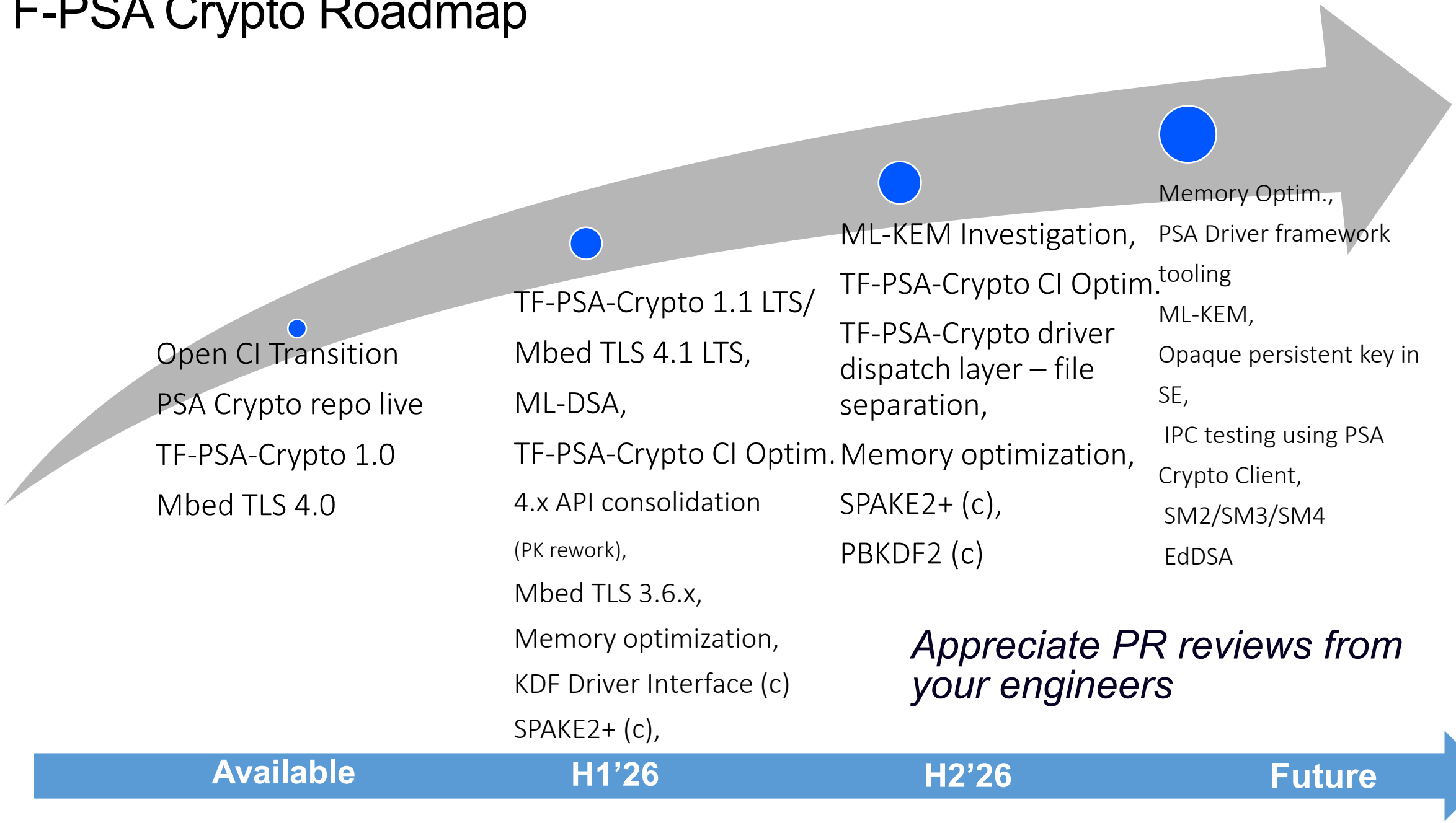
Risks and Bottlenecks

- Security issues
  - Higher volume than usual (bug bounty, 1.0, proliferation of AI tools)
  - Not predictable, taking up teams' time and means risk for delivery timelines
  - OSTIF audit

- Reviews
  - Review continues to be a challenge, there are much more contributions than what we can take
  - Appreciate review bandwidth from engineers from member companies
    - They don't necessarily have to be cryptographers or security engineers
  - We are working on a process to support people becoming trusted reviewers
  - Becoming a trusted reviewer and contributing reviews is
    - the only way to contribute features not on the roadmap
    - a way to expedite features on the roadmap

© 2026 Arm

TF-PSA Crypto Roadmap



Appreciate PR reviews from your engineers

arm

© 2026 Arm

arm

Tack
ಧನ್ಯವಾದಗಳು
Merci
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Thank you
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు
Köszönöm